RECEIVED
CENTRAL FAX CENTER

OCT 1 1 2006



## REMARKS

**Claim Rejection Under 35 U.S.C. § 103**

In the Final Office Action, the Examiner rejected claims 1, 2, 4, 5, 7–9, 12, 13, 16–19 under 35 U.S.C. 103(a) as being unpatentable over Jardin (USPN 6,681,327) in view of Lockhart et al. (USPN 5,841,873). The Examiner rejected claims 6, 14, 15, and 20 under 35 U.S.C. 103(a) as being unpatentable over Jardin in view of Lockhart and in further view of Lin et al. (USPN 6,052,785). Applicant respectfully traverses the rejection.

As a preliminary comment, Applicant thanks the Examiner for his clarifying remarks on pp. 2-4 of the Office Action in the response to Applicant's arguments. Applicant better understands the Examiner position. Applicant traverses the rejection and submits that the claims in their current form are patentably distinct from Jardin in view of Lockhart. Applicant respectfully requests the Examiner reconsider the Final Office Action in view of the following remarks.

Applicant's independent claim 1 is directed to a method in which an intermediary device negotiates a secure communications session with a client apparatus, and receives encrypted packet application data for a security record that has a length greater than a packet length associated with multiple data packets. In the Final Office Action, paragraph 6 of pg. 3, the Examiner clarified his position that he is interpreting the elements of claim 1 that recite a security record that has a length greater than a packet length so as to encompass an entire "security session that spans multiple packets." The Examiner then clarified that the cited portions of Jardin teaches a secure session that spans multiple packets, where the entire secure session is construed as a security record. Presumably the Examiner is referring the secure session maintained between the client and the server broker in Jardin since this is the only session from which encrypted data is received by an intermediate device from a client apparatus, as required by claim 1.

Assuming, hypothetically, that an entire SSL session could be "reasonably construed" as a single security record, as asserted by the Examiner, Jardin in view of Lockhart fail to teach or suggest features of Applicant's independent claim 1.

First, claim 1 requires the steps of forwarding unauthenticated data from the intermediate device to the server, and authenticating the security record on receipt of the final packet of the security record. Based on the Examiner's interpretation that the element "security record" covers Jardin's SSL session, then for this limitation Jardin in view of Lockhart would need to teach or suggest that data from the SSL session between the client and the server broker is sent from the server broker to the server, and that the data is authenticated upon receiving the last packet of the session. This construction of Applicant's claim and the prior art is nonsensical.

Applicant's claim 1 literally requires authenticating the security record on receipt of the final packet of the security record. Waiting until the last packet of the entire session before "authenticating the security session" (as would be required by the Examiner's construction of a security record) makes no sense whatsoever. The Examiner's interpretation that the claim element "security record" covers Jardin's SSL session would require that Jardin in view of Lockhart suggest that the SSL session is authenticated upon receiving the last packet of the session, which is clearly incorrect.

Second, claim 1 requires forwarding decrypted, unauthenticated application data to the server via the secure network. With respect to these elements, the Examiner stated his position in the Office Action, paragraph 9, pg. 3, as "Jardin discloses redirecting decrypted packets for fulfillment. ... Jardin discloses that the server broker decrypts the packets and forwards them to the server for fulfillment (i.e., authentication)." Thus, the Examiner position is that in Jardin, the server performs the authentication function for the secure record.

In response, Applicant first points out that claim 1 recites a "method performed on an intermediary device." The Examiner's position that the Jardin server broker decrypts the packets and then the server "authenticates" the decrypted packets by fulfilling the transaction is irrelevant to the elements of claim 1 that require the authentication be performed by the intermediate device.

Furthermore, Jardin makes clear that server broker (i.e., the intermediate device) operates as a proxy for the server. As a proxy, the server broker maintains a first SSL session between the broker and the client and a second session (either unsecure as TCP or secure using SSL/TCP) between the broker and the server. FIG. 2 and the related text of Jardin illustrate the broker establishing the secure SSL session with the client. FIG. 3 and the related text show the broker

establishing a separate session between the broker and the server for communicating the decrypted data to the server. This may be a secure SSL session (see block 334) or unsecure (see block 344).

The point is that the data sent from the server broker to the server must be "authenticated" data with respect to the SSL session between the client and the server broker. Specifically, the server broker operates as an endpoint for the SSL session between the broker and the client, which is typical for SSL proxies, and utilizes a separate session to send the data to the server. Contrary to the Examiner's position, although not mentioned by Jardin, any authentication performed with respect to this SSL session and/or the SSL records received from the client would have to be performed by the server broker in order for the server broker to act as a proxy. The result of this is that the data sent from the intermediate device (the server broker) to the server in Jardin has already been authenticated by the Jardin server broker since the server broker operates as a proxy and terminates (acts as an endpoint for) the SSL session with the client. In other words, in Jardin, the server broker is the only device that can authenticate the SSL data received from the client by the SSL session between the client and the server broker. The backend server is not involved in this session and would certainly not authenticate the SSL records communicated via that session. Jardin makes clear that the packets received from the SSL session with the client are decrypted and then send to the server using an entirely different session. The Examiner's assertion that "unathenticated data" for a security record is somehow forwarded to the server by the server broker for authentication with respect to that security record is incorrect.

Third, the Examiner's interpretation of Applicant's claim element of a "security record" as encompassing and entire SSL session of Jardin is erroneous in view of well established principles of claim construction. The Examiner's construction overlooks the fact that claim 1 specifically recites a "secure communication session" between the intermediate device and the client separately from a "security record" received from the client. These are two distinct elements of claim 1 that the Examiner has impermissibly merged.

Further, the Examiner's excuse for such his interpretation is based on the assertion that the Applicant is being his own lexicographer. Specifically, in paragraphs 5-6 at pp. 2 of the Office Action, the Examiner states that Jardin "does not use the same terminology" as the

Applicant and that the Applicant is attempting to define the term security record with an "uncommon definition." This could not be further from the truth. Jardin and Applicant's specification and claims both refer to SSL sessions, although Jardin does not mention the underlying SSL records. It is well known throughout the networking industry that the SSL protocol, as described in Jardin, exchanges secure data in an SSL session by a series of "secure records." For example, Wikipedia states the following:

> *The SSL protocol exchanges **records**; each record can be optionally compressed, encrypted and packed with a message authentication code (MAC). Each record has a content_type field that specifies which upper level protocol is being used.... TLS/SSL have a variety of security measures:*
>
> > *Numbering all the records and using the sequence number in the MACs.*
> > *Using a message digest enhanced with a key (so only with the key can you check the MAC). This is specified in RFC 2104).*[1]

As further evidence,

> *The SSL protocol includes two sub-protocols: the SSL record protocol and the SSL handshake protocol. The SSL record protocol defines the format used to transmit data. The SSL handshake protocol involves **using the SSL record protocol to exchange a series of messages** between an SSL-enabled server and an SSL-enabled client when they first establish an SSL connection.*[2]

As additional evidence, Cisco describes the SSL record protocol as forming records to be transmitted as follows:

> The SSL Record Protocol provides two services for SSL connections: confidentiality, by encrypting application data; and message integrity, by using a message authentication code (MAC). The Record Protocol is a base protocol that can be utilized by some of the upper-layer protocols of SSL. One of these is the handshake protocol which, as described later, is used to exchange the encryption and authentication keys. It is vital that this key exchange be invisible to anyone who may be watching this session.
>
> The Record Protocol takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment. Received data is decrypted, verified, decompressed, and reassembled and then delivered to the calling application, such as the browser.[3]

---

[1] www.wikipedia.org
[2] http://www.faqs.org/docs/Linux-HOWTO/SSL-RedHat-HOWTO.html
[3] http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html

Thus, it is clear that the Examiner's redefinition of the Applicant's claim term "security record" to read on an entire SSL session, as described by Jardin, is inconsistent with the well-known use of the term. One of ordinary skill would not construe an SSL session as an individual security record, as suggested by the Examiner. It is clear that Applicant is not setting out some "uncommon definition," as suggested by the Examiner. Further, it is the Examiner's interpretation of the term "security record" that is inconsistent with Jardin's description of an SSL session and the well-known use of the term within industry. Moreover, as discussed above, the Examiner's interpretation contradicts other elements cited within Applicant's claims and effectively erases other elements from the claims as being duplicative, which is impermissible.

Finally, Applicant points out that dependent claim 8 specifically recites that the data of the security record is SSL encrypted data. This, therefore requires that the "security record" of claim 1 is an SSL security record. Thus, the Examiner's construction of "security record" with respect to claim 8 would require that the SSL security record constitutes an entire SSL session. As demonstrated above, it is well known that an individual SSL security record is not the same as an SSL session..

For at least these reasons, Jardin in view of Lockhart et al. and in further view of Lin fails to establish a prima facie case for non-patentability of Applicants' claims under 35 U.S.C. 103(a). Withdrawal of this rejection is requested. Applicant traverses the rejection with respect to the other claims for reasons set forth in Applicant's previous responses, hereby incorporated by reference.

## CONCLUSION

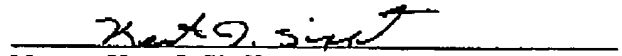
All claims in this application are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application..

Application Number 09/900,493
Responsive to Office Action mailed August 11, 2006

Date:

October 11, 2006

By:



SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102

Name: Kent J. Sieffert
Reg. No.: 41,312